CALCULATIONS: QUANTUM COMPUTING AND BITCOIN

1) QUANTUM SPEEDUP IN MINING (Grover's Algorithm)
Classical operations (example): 2^16 = 65,536
Quantum operations (Grover): √(2^16) = 256
Speedup: 256× faster

Calculation with real difficulty:
Classical attempts: 2^16 = 65,536
Quantum attempts: 2^8 = 256
Real speedup: ~256×

---

2) IMPACT ON BITCOIN ISSUANCE
Normal issuance:
- Blocks per day: 144
- BTC per block: 3.125
- BTC per day: 450.00
- BTC per year: 164,250.00

Scenario with a quantum miner (256× speedup):
- Time per block: 2.3 seconds
- Blocks per day (before difficulty adjusts): 36,864
- BTC per day (before difficulty adjusts): 115,200.00

⚠️ **But difficulty adjusts every 2016 blocks (~2 weeks).**
⚠️ **During that window there would be extreme centralization.**

---

3) BREAKING ECDSA (Shor's Algorithm)
ECDSA key: 256 bits
Classical operations: 2^128 (infeasible)
Quantum (Shor): O(n^3) ≈ 256^3 = 16,777,216

Estimated time (with 1M qubits at 1 GHz):
- 0.02 seconds
- 0.00 minutes

Bitcoins at risk:
- BTC with exposed public keys: 4,000,000
- Approximate value ($60,000/BTC): $240,000,000,000
- In trillions: $0.24T

---

4) QUANTUM HARDWARE REQUIREMENTS
For quantum mining:
- Transactions per block: 3,000
- n = $\log_2(3{,}000)$ ≈ 12
- Required logical qubits: 256n + 256 + 32 + n
- **Total:** 3,372 logical qubits

For breaking ECDSA:
- Traditional estimate: 2,000,000 qubits
- New estimate (2025): 700 qubits
- **Reduction:** 2,857× easier

---

5) CURRENT STATE vs REQUIRED
Current qubits (largest computer): 1,000

Estimated time until threat:
- Mining (3,372 qubits): ~4 years
- ECDSA (700 qubits): ~<1 year
- Traditional ECDSA (2,000,000 qubits): ~22 years

---

6) RISK ANALYSIS
Probability of a successful attack:
- Short term (1–2 years): **LOW**
- Medium term (3–5 years): **MODERATE** (if the new estimate is correct)
- Long term (5–10 years): **HIGH**

Potential impact:
- Breaking ECDSA: **CATASTROPHIC**
- Mining centralization: **SEVERE**
- Loss of confidence: **IRREVERSIBLE**

CONCLUSION
The quantum threat to Bitcoin is real and growing.